

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-102951

(43)Date of publication of application : 02.04.2004

(51)Int.Cl. G06F 15/00
G06F 12/14
G06F 17/30
G09C 1/00
H04L 9/32

(21)Application number : 2002-267551

(71)Applicant : HITACHI LTD

(22)Date of filing : 13.09.2002

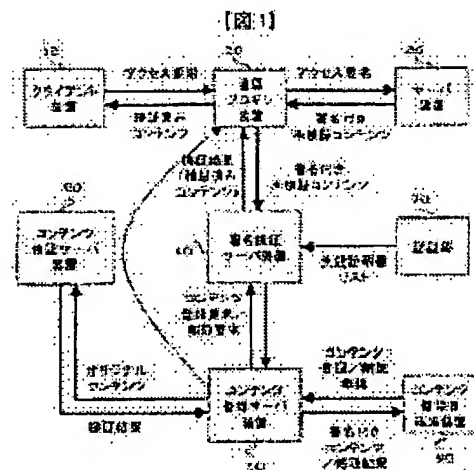
(72)Inventor : TAKESHIMA YOSHIAKI
NAKAHARA MASAHIKO

(54) NETWORK SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To rapidly verify whether if there will be a problem to send contents provided by a server device to a client device in relay of communication between the client device and the server device.

SOLUTION: In regard to contents exchanged via a network, a contents creator or provider registers contents precedently verified by a contents verifying server device 60 in a contents registering server device 50 and receives issuance of a signature, and then the contents are stored in the server device 30. In contents download, a communication proxy device 20 transfers the contents to a signature verifying server device 40 to receive verification of the signature, and unaltered contents are sent to the client device 10.



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2004-102951

(P2004-102951A)

(43) 公開日 平成16年4月2日 (2004.4.2)

(51) Int. Cl.⁷

F I

テーマコード (参考)

G06F 15/00

G06F 15/00 330A

5B017

G06F 12/14

G06F 12/14 310Z

5B075

G06F 17/30

G06F 17/30 110E

5B085

G09C 1/00

G09C 1/00 640D

5J104

H04L 9/32

H04L 9/00 675B

審査請求 未請求 請求項の数 15 O L (全 25 頁) 最終頁に続く

(21) 出願番号

特願2002-267551 (P2002-267551)

(22) 出願日

平成14年9月13日 (2002.9.13)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(74) 代理人 100075096

弁理士 作田 康夫

(72) 発明者 竹島 由晃

神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所システム開発研究所
内

(72) 発明者 中原 雅彦

神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所システム開発研究所
内

Fターム (参考) 5B017 AA08 CA16

最終頁に続く

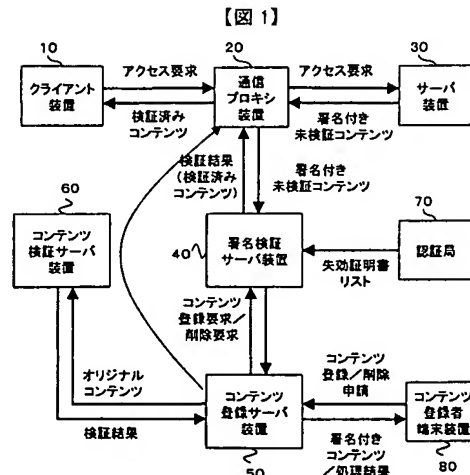
(54) 【発明の名称】 ネットワークシステム

(57) 【要約】

【課題】 クライアント装置とサーバ装置間の通信の中継において、サーバ装置が提供するコンテンツをクライアント装置に送信しても問題ないかを高速に検証する。

【解決手段】 ネットワークを介してやりとりされるコンテンツに対し、コンテンツ作成者もしくは提供者は事前にコンテンツ検証サーバ装置60が検証したコンテンツをコンテンツ登録サーバ装置50に登録して署名の発行を受けた後、該コンテンツをサーバ装置30に格納し、コンテンツダウンロード時に、通信プロキシ装置20は該コンテンツを署名検証サーバ装置40に転送して署名の検証を受け、改竄されていないコンテンツをクライアント装置10に送信する。

【選択図】 図1



【特許請求の範囲】

【請求項1】

サーバ装置に対しアクセス要求を発行するクライアント装置と、
クライアント装置からのアクセス要求を受信してコンテンツを配信するサーバ装置と、
コンテンツを受信すると該コンテンツに対して付加的处理を行った後に送信元に応答する
アプリケーションサーバ装置と、
前記クライアント装置と前記サーバ装置間のデータ通信を中継する通信プロキシ装置とを
備え、
前記通信プロキシ装置は、
前記クライアントから前記アクセス要求を受信して、前記サーバ装置に転送し、前記サー
バ装置から前記コンテンツを受信する通信中継処理部と、
前記通信中継処理部からコンテンツを受信し、所定のフォーマットに従うメッセージに再
構築して前記アプリケーションサーバ装置に送信し、前記アプリケーションサーバ装置で
付加処理された結果を受信するアプリケーションサーバ呼び出し処理部と、を備え、
前記通信中継処理部は、前記結果に基づいたデータを前記クライアント装置へ送信する
ネットワークシステム。

10

【請求項2】

請求項1に記載のネットワークシステムにおいて、
前記通信プロキシ装置は、
前記アプリケーションサーバ装置に前記コンテンツを転送する条件と、前記コンテンツを
転送するために必要な前記アプリケーションサーバ装置の情報を記憶する転送制御データ
ベースを備え、
前記通信中継処理部は、
前記アクセス要求と前記コンテンツの内容が、前記転送制御データベースに記憶されてい
る条件を満足する場合に、前記アプリケーションサーバ呼び出し処理部に前記コンテンツ
を渡す
ネットワークシステム。

20

【請求項3】

請求項1に記載のネットワークシステムにおいて、
前記通信中継処理部は、
前記サーバ装置から応答された前記コンテンツをキャッシュとして記憶し、
当該キャッシュとして記憶しているコンテンツを対象とするアクセス要求を前記クライア
ント装置から受信した場合に、前記コンテンツと共に記憶しているかもしくは前記通信プ
ロキシ装置に予め設定されている、有効期限内であれば、前記キャッシュとして記憶され
ているコンテンツを前記クライアント装置に応答する
ネットワークシステム。

30

【請求項4】

請求項3に記載のネットワークシステムにおいて、
前記通信中継処理部は、
前記アプリケーションサーバ装置から応答された前記付加処理結果に応じて、前記サー
バ装置から応答されたコンテンツ、もしくは前記アプリケーションサーバ装置から応答され
た付加処理済みデータ、もしくは、キャッシュとして記憶しているコンテンツ、もしくは
エラーメッセージのいずれかを前記クライアント装置に応答する
ネットワークシステム。

40

【請求項5】

請求項3に記載のネットワークシステムにおいて、
前記通信中継処理部は、前記アプリケーションサーバ装置から受信した付加処理され
たコンテンツを、または付加処理されたコンテンツのネットワーク上の位置情報に従いネ
ットワーク経由で取得したコンテンツを、キャッシュとして記憶する
ネットワークシステム。

50

【請求項6】

請求項5に記載のネットワークシステムにおいて、
コンテンツ管理者からコンテンツを受け付ける、コンテンツ登録サーバ装置と、
前記コンテンツ登録サーバ装置にコンテンツを登録するためのインタフェースとなるプログラムが動作するコンテンツ登録者端末装置と、
前記コンテンツ登録サーバ装置からコンテンツを受信して所定の方法で当該コンテンツの内容をチェックする、コンテンツ検証サーバ装置と、
を備え、
前記コンテンツ登録サーバ装置は、前記コンテンツ検証サーバ装置が前記コンテンツが所定の条件を満たしている場合に、前記コンテンツ登録者端末から受信したコンテンツに対して、署名を付加した署名付きコンテンツを作成する
ネットワークシステム。 10

【請求項7】

請求項6に記載のネットワークシステムにおいて、
前記コンテンツ登録サーバ装置は、
前記コンテンツを一意に特定するコンテンツIDに基づいて前記署名を生成する署名生成処理部と、
前記署名を生成するための秘密鍵、及び対応する公開鍵の公開鍵証明書を管理する鍵管理部と、
前記コンテンツIDを発行し、前記署名付きコンテンツを登録情報データベースに登録する登録情報管理部とを備える
ネットワークシステム。 20

【請求項8】

請求項7に記載のネットワークシステムにおいて、
前記コンテンツ登録サーバ装置は、前記通信プロキシ装置に前記署名付きコンテンツのキャッシュを依頼する
ネットワークシステム。

【請求項9】

請求項6に記載のネットワークシステムにおいて、
前記コンテンツ検証サーバ装置は、複数のセキュリティレベルを管理するデータベースを
備え、
前記セキュリティレベル別に前記コンテンツ検証を行う
ネットワークシステム。 30

【請求項10】

請求項6に記載のネットワークシステムにおいて、
マスタとなる前記コンテンツ登録サーバ装置とスレーブとなる一つ以上の前記コンテンツ登録サーバを備え、
マスタとなる前記コンテンツ登録サーバ装置は、スレーブとなるコンテンツ登録サーバ装置と通信を行い、
それぞれのコンテンツ登録サーバが備えるデータベースの同期を行う
ネットワークシステム。 40

【請求項11】

請求項6に記載のネットワークシステムにおいて、
前記アプリケーションサーバ装置は、前記署名付きコンテンツの署名を検証する署名検証サーバ装置であって、
前記サーバ装置は、前記コンテンツ登録サーバ装置によって署名を付加された前記署名付きコンテンツを記憶し、
前記通信プロキシ装置は、
前記サーバ装置から受信した前記署名付きコンテンツを前記署名検証サーバ装置へ転送し、
、

検証結果に応じて、前記署名付きコンテンツをクライアント装置に送信するかどうかを決定する

ネットワークシステム。

【請求項 1 2】

請求項 1 1 に記載のネットワークシステムにおいて、

前記署名検証サーバ装置は、

前記通信プロキシ装置より受信した未検証の署名付きコンテンツから署名を取得する署名取得処理部と、

前記署名を検証するために用いる公開鍵証明書の有効性を検証する証明書検証処理部と、公開鍵証明書の有効性検証に用いる失効証明書リストを管理する失効証明書リストデータベースと、

署名を検証するための署名検証処理部と、

署名に含まれるコンテンツ ID に対応する登録情報を記憶する登録情報データベースと、前記コンテンツ ID に対応する登録情報を管理するための登録情報管理処理部とを備えるネットワークシステム。

10

【請求項 1 3】

請求項 1 2 に記載のネットワークシステムにおいて、

前記署名検証サーバ装置は、前記コンテンツ登録サーバ装置と通信を行い、前記登録情報データベースの同期を行う

ネットワークシステム。

20

【請求項 1 4】

請求項 1 1 に記載のネットワークシステムにおいて、

前記通信プロキシ装置は、前記検証結果が「有効」であれば検証済みの前記署名付きコンテンツを、署名付きのまま、もしくは署名を除去して前記クライアント装置に送信し、「無効」であればエラーを送信する

ネットワークシステム。

【請求項 1 5】

請求項 1 1 に記載のネットワークシステムにおいて、

第 1 のコンテンツに対する署名を第 2 のコンテンツに付加しておき、

前記署名検証サーバ装置が前記第 2 のコンテンツを検証する時に、付加されている前記第 1 のコンテンツの署名を保存しておき、

30

前記第 1 のコンテンツの検証時に、前記保存していた前記第 1 のコンテンツの署名を用いて検証する

ネットワークシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、サーバ装置上にあるコンテンツを、通信回線で接続したクライアント端末からアクセスするネットワークシステムにおいて、サーバ装置とクライアント端末間の通信を中継代行する通信プロキシ装置、及び該通信プロキシ装置を用いたシステムに関する。

40

【0002】

【従来の技術】

HTTP (Hypertext Transfer Protocol) と呼ぶプロトコルを用いて、実行プログラムや音楽、動画像ファイルをダウンロードして実行、再生するといった利用形態が普及している。このような利用形態においては、ユーザ端末に対するセキュリティの確保は大きな課題である。例えば、悪意のある第三者が、インターネット上にある Web サーバに侵入し、サーバ上にあるコンテンツ (例えば、動画像ファイルや実行プログラムなど) データを、コンピュータウィルスプログラムに改竄することがある。そうすると、ユーザが知らずにそのプログラムをダウンロードしてしまい、ユーザ端末でそのプログラムを動作させてしまうことによって、ユーザ端末に記憶されているデータ

50

が破壊されてしまったり、秘匿すべきユーザの大事な個人情報が悪意のある第三者に勝手に送信されてしまう、といった問題が発生する。その対策として、データを検証して、コンピュータウィルスを検知し除去するウィルス検知プログラムを用いる方法がある。この対策方法は主に次の二つの形態で運用される。

【0003】

一つは、ユーザ端末もしくはWebサーバでウィルス検知プログラムを動作させる方法である。もう一つは、ネットワークの通信プロキシ装置、例えばプロキシサーバやファイアウォール上で動作させ、ダウンロード中のコンテンツに対してリアルタイムにウィルスを検知する方法である。Webプロキシとは、サーバ装置とクライアント装置間でWeb通信を中継代行する技術であり、これに関しては、非特許文献1で詳しく述べられている。本方法は、ネットワーク上でウィルス検知を行うため、インターネット接続サービスを提供している通信キャリアが、ユーザに対してセキュリティサービスを提供するのに適している。

10

【0004】

【非特許文献1】

R. Fielding 他、RFC2616「Hypertext Transfer Protocol — HTTP/1.1」、[online]、1999年6月、The Internet Society、[2002年8月27日検索]、インターネット<URL: <http://www.ietf.org/rfc/rfc2616.txt>>、1.3節、1.4節

20

【0005】

【発明が解決しようとする課題】

前者の方法では、ネットワークに接続されている全てのユーザ端末にウィルス検知プログラムを導入することが難しい。また、ユーザ端末が携帯電話である場合には、ウィルス検知プログラムを動作させることが出来ない。また、サーバ側で実行させる場合でも、ウィルス検知済みのデータが、ネットワークを流れる途中でウィルスに感染する可能性がある。

【0006】

また、後者の方法では、ネットワークトラフィックが集中する通信プロキシ装置が負荷の重いウィルス検知処理を行うため、通信プロキシ装置自体の処理性能が非常に低くなる。ウィルス検知プログラムを通信プロキシ装置に接続している別のサーバ装置で動作させ、通信プロキシ装置との間でデータの交換を行う方法も提案されているが、この方法でも、ウィルス検知プログラムが動作しているサーバ装置が処理性能のボトルネックとなる点では同じである。

30

【0007】

上記のように、クライアント装置がサーバ装置からダウンロード中のコンテンツに対し、サーバ装置ではなく、ネットワークの中継装置で付加的処理をおこなおうとすると、その処理負荷の重さが課題となる。

【0008】

【課題を解決するための手段】

本発明は、クライアント装置とサーバ装置間に備えられた通信中継装置（通信プロキシ装置と称する）が、クライアント装置とサーバ装置間のデータ通信を中継する通信中継処理部と、通信中継処理部がサーバ装置から受信したコンテンツを所定のフォーマットに従うメッセージに再構築してアプリケーションサーバ装置に転送し、アプリケーションサーバ装置が付加処理を行い応答したデータを受信するアプリケーションサーバ呼び出し処理部とを備えることを特徴とする。これにより、クライアント装置がダウンロード中のコンテンツに対し、サーバ装置ではなく、ネットワークの中継装置が付加的処理を指示することが可能となる。

40

【0009】

ここで、通信プロキシ装置は、アプリケーションサーバ装置にコンテンツを転送する条件

50

、及びコンテンツデータを転送するために必要なアプリケーションサーバ装置の情報を設定及び記憶する転送制御データベースを備え、通信中継処理部は、アクセス要求及びコンテンツの記述内容を解析し、転送制御データベースに記憶されている条件を満たしている場合に、アプリケーションサーバ装置に転送する。

【0010】

アプリケーションサーバ呼び出し部は、アプリケーションサーバ装置から応答された処理結果を解析して、サーバ装置から応答されたコンテンツ、もしくはアプリケーションサーバ装置から応答されたデータ、もしくは過去に通信プロキシ装置にキャッシュとして記憶されているコンテンツ、もしくはエラーメッセージをクライアント装置に応答する。これにより、クライアント装置へ適切な応答を行うことができるので、アプリケーションサーバ装置と通信プロキシ装置間のデータ通信量を減少させることができる。また、クライアント装置やサーバ装置にはなんら変更を加えることなく、コンテンツに対して付加的処理を加えることができる。

10

【0011】

また、通信中継処理部は、アプリケーションサーバ装置からコンテンツ本体のデータを受信するか、もしくはURL情報を受信してそのコンテンツをネットワーク経由で取得することにより、取得したコンテンツをキャッシュとして記憶する。これにより、アプリケーションサーバ装置が提供する付加的処理に関連する特定のコンテンツを高速にクライアント装置に応答したい場合に、アプリケーションサーバ装置が通信プロキシ装置に対して、クライアント装置からのアクセスがある前にそのコンテンツをキャッシュするように指示

20

【0012】

本発明のネットワークシステムは、例えば、アプリケーションサーバ装置として、コンテンツ作成者もしくは提供者（コンテンツ管理者ともいう）から受け付けたコンテンツの登録申請に応じて、ウィルス検知など内容チェックを行ったコンテンツに電子署名（以下、単に署名という）を付加してデータベースに登録するコンテンツ登録サーバ装置や、登録申請されたコンテンツについてウィルス検知など内容をチェックするコンテンツ検証サーバ装置や、署名を検証する署名検証サーバ装置を備える。

【0013】

本発明によれば、サーバ装置は上記署名付きコンテンツを記憶し、通信プロキシ装置は、クライアント装置の要求に従いダウンロードした署名付きコンテンツを、署名検証サーバ装置に転送する。署名検証サーバ装置は、コンテンツに付加されている署名の有効性を確認した後、検証結果を通信プロキシ装置に回答し、通信プロキシ装置は、検証結果が有効であればコンテンツをクライアント装置に回答し、無効であればエラーを回答する。これにより、コンテンツの内容を前もって検証しておき、ダウンロード時にはコンテンツに付加された署名のチェックのみで、コンテンツ内容の検証を行うことができる。そのため、クライアント装置に対して内容が検証されたコンテンツを迅速に配信することが可能となる。

30

【0014】

なお、署名の発行と検証には、本ネットワークシステムが記憶する秘密鍵及び公開鍵証明書を用いる。

40

【0015】

すなわち、サーバ装置からユーザ端末へ送信される署名付きコンテンツを中継する通信プロキシ装置が、当該署名付きコンテンツを前述のアプリケーションサーバ装置としての署名検証サーバ装置に転送することにより、ユーザ端末にコンテンツ検証プログラムを動作させることを必要とせず、またネットワーク途中での改竄を防ぎ、高い処理性能を保ちながら、セキュリティを確保する。

【0016】

また、コンテンツ登録サーバ装置は、コンテンツ登録処理を行う際に、通信プロキシ装置に対して検証済みコンテンツをキャッシュさせる機能を備える。これにより、クライアン

50

ト装置から登録コンテンツに対してアクセスがあった場合に、安全なコンテンツを迅速に送信することができる。

【0017】

また、コンテンツ検証サーバ装置は、複数のセキュリティレベルをテーブルとして管理することにより、契約などに基づいて設定されたセキュリティレベル別にコンテンツ検証を行うことができる。

【0018】

また、署名検証サーバ装置は、署名付きコンテンツを受信すると、署名の検証によるコンテンツ改竄チェックと、さらに署名中のコンテンツIDをデータベースで検索することによるコンテンツ内容の有効性チェックを行うことで、コンテンツをクライアント装置に

10

【0019】

通信プロキシ装置から署名検証の処理を別サーバ装置として分離することにより、処理負荷の重い署名検証処理を、トラフィックの集中する通信プロキシ装置で行わず、通信プロキシ装置の処理速度を向上させることができる。また、署名検証処理を行うソフトウェアの新規機能追加や変更等を、通信プロキシ装置を停止させることなく、署名検証サーバ装置の交換と通信プロキシ装置の転送設定の変更だけを行うことが可能になり、保守運用が容易になる。

【0020】

また、署名検証サーバ装置とコンテンツ登録サーバ装置は、コンテンツ登録サーバ装置群で共通管理しているデータベースの同期を行うことにより、本発明のネットワークシステム内部でコンテンツ登録情報を共有し、不整合を発生させることなく管理することができる。

20

【0021】

さらに、本発明のコンテンツ検証方法は、複数のコンテンツを対としてコンテンツ登録サーバ装置に登録することで、クライアント装置から対としてダウンロードされているかを検証することができる。具体的には、第1のコンテンツの署名を第2のコンテンツに付加しておき、署名検証サーバ装置は第2のコンテンツを検証する時に、付加されている第1のコンテンツの署名を保存しておく。次に第1のコンテンツを検証する時には、保存している第1のコンテンツの署名を用いて検証する。これにより、第1のコンテンツと第2のコンテンツとが、予め登録された対としてダウンロードされたことを検証することができる。片方のコンテンツが、もう片方のコンテンツをダウンロードした後にダウンロードされた時のみ有効、といった制御が可能となる。

30

【0022】

なお、本発明において、コンテンツとは、文書ファイルやマルチメディアデータ（例えば、音楽ファイルや動画ファイル）、または実行プログラムなどのデジタルデータを指す。

【0023】

【発明の実施の形態】

本発明の実施形態に関わる各装置は、例えば図14に示すような、CPU11と、メモリ12と、CD-ROMやDVD-ROM等の着脱可能で可搬性を有する記憶媒体18から情報を読み出す読み取り装置13と、ネットワーク9を介して相手装置と通信を行うための通信装置14と、HDD等の外部記憶装置15と、キーボードやマウスやディスプレイなどの入出力装置16と、を備えた一般的なコンピュータシステムにおいて、CPU11がメモリ12上にロードされた所定のプログラムを実行することにより実現することができる。

40

【0024】

以下に、本発明の第一の実施の形態を、図を用いて説明する。

【0025】

図1は、本発明の一実施形態が適用されたネットワークシステムの概略構成を示す図であ

50

る。

【0026】

本実施の形態では、本ネットワークシステムは、クライアント装置10及びサーバ装置30と、クライアント装置10とサーバ装置30間のデータ通信を中継する通信プロキシ装置20と、コンテンツに付加された署名を用いてコンテンツをクライアント装置10に送信しても良いかどうかを検証する署名検証サーバ装置40と、コンテンツ作成者や保持者などのコンテンツ管理者から前もってコンテンツを受け付けてコンテンツに署名を生成するコンテンツ登録サーバ装置50と、コンテンツ登録サーバ装置50が受信したコンテンツの内容をチェックするコンテンツ検証サーバ装置60と、署名検証サーバ装置40が署名を検証する際に用いる公開鍵証明書のうち失効した公開鍵証明書のリストを配布する認証局70と、コンテンツ管理者がコンテンツ登録サーバ装置50にコンテンツを登録するのに用いる端末であるコンテンツ登録者端末80とを備え、各装置はネットワーク9を介して接続されている。

10

【0027】

クライアント装置10及びサーバ装置30は、一台以上の通信プロキシ装置20を介して接続している。また、通信プロキシ装置20は、署名検証サーバ装置40と接続し、署名検証サーバ装置40は、コンテンツ登録サーバ装置50及び認証局70に接続している。コンテンツ登録サーバ装置50は、コンテンツ検証サーバ装置60及びコンテンツ登録者端末装置80に接続している。

【0028】

クライアント装置10は、Webブラウザなどの既存のWebクライアントアプリケーションが動作している。クライアント装置10が、サーバ装置30が記憶する文書データや動画像データ、プログラムファイルなどのコンテンツをダウンロードする際、サーバ装置30にコンテンツ送信要求を示すメッセージ（アクセス要求）を送信することにより、応答データ（コンテンツ）を受信する。

20

【0029】

サーバ装置30は、Webサーバプログラムが動作しており、クライアント装置10からアクセス要求を受信すると、要求されたコンテンツをクライアント装置10に送信する。本実施の形態では、サーバ装置30は図9に示す、署名付きコンテンツ31を記憶する。

【0030】

署名付きコンテンツ31は、クライアント装置10からのアクセス要求がある前に、予めコンテンツ登録者端末80からコンテンツ登録サーバ装置50に登録され、コンテンツ検証サーバ装置60で内容をチェックされて、クライアント装置10がダウンロードしてもよいものとして署名を付加されたものである。なお、本実施の形態における署名は、ハッシュ関数を用いた公開鍵暗号による署名である。

30

【0031】

図9に示した署名付きコンテンツ31は、文書や動画、実行プログラムなどのオリジナルコンテンツ311と、該オリジナルコンテンツ311の有効性を検証するために用いる署名312とを備える。署名312は、署名情報3121と、署名情報3121を秘密鍵で暗号化した署名値3122と、署名値3122を復号化するために必要な公開鍵を含む公開鍵証明書3123とを含む。署名情報3121は、ハッシュ関数のアルゴリズムなどを示す署名方法3124と、本システムが各コンテンツに対して一意に割り振ったID情報であるコンテンツID3125と、コンテンツデータにハッシュ関数を作用させることによって計算した、コンテンツの特徴値（ダイジェスト値）3126とを含む。

40

【0032】

図1の通信プロキシ装置20は、クライアント装置10からサーバ装置30宛に送られるアクセス要求と、それに対する応答コンテンツを中継する機能（中継機能）を備える。宛先となるサーバ装置30の情報（ホスト名やIPアドレスなど）は、アクセス要求中に記述されている、コンテンツのURL情報に含まれている。

【0033】

50

また、通信プロキシ装置 20 は、中継した応答コンテンツをキャッシュとして記憶するキャッシュ機能を備える。

【0034】

さらに、通信プロキシ装置 20 は、サーバ装置 30 から応答された署名付きコンテンツ 31 が、予め設定されている条件（当該コンテンツの URL や拡張子、ファイルタイプ等）を満たした際に、署名検証サーバ装置 40 に転送して署名検証を依頼し、検証結果に問題が無ければコンテンツをクライアント装置 10 に送信する。

【0035】

通信プロキシ装置 20 と署名検証サーバ装置 40 間の通信は、例えば HTTP や ICAP などの通信プロトコルを用いて良い。

10

【0036】

署名検証サーバ装置 40 は、通信プロキシ装置 20 から送信されてきた署名付きコンテンツ 31 を受信すると、署名を検証してコンテンツが改竄されていないことを確認し、結果を通信プロキシ装置 20 に送り返す。

署名検証サーバ装置 40 は、認証局 70 から、署名を検証する際に用いる公開鍵証明書のうち、失効した公開鍵証明書のリストを受信して記憶しておき、署名付きコンテンツ 31 受信時に、公開鍵証明書と失効証明書リストを照らし合わせて公開鍵の有効性を検証する。

【0037】

また、署名検証サーバ装置 40 は、コンテンツ ID 3125 毎に、そのコンテンツの有効性を表す情報を登録情報データベース 45 として記憶する。

20

【0038】

コンテンツ登録サーバ装置 50 は、署名発行とコンテンツ登録管理を行なう。

【0039】

署名発行機能は、コンテンツ登録者端末装置 80 からのコンテンツ登録を受け付けてコンテンツを受信し、受け付けたコンテンツをコンテンツ検証サーバ装置 60 に送信して検証結果を受信し、コンテンツの内容に問題が無いことを確認して、そのコンテンツに対する署名を生成してコンテンツに付加し、コンテンツ登録者端末 80 に応答する機能である。

【0040】

例えば、実行プログラムファイルの登録を受け付けた場合は、実行プログラム中にコンピュータウィルスが含まれていないか、プログラムが使用するために読み込んでいるクラスライブラリがクライアント端末 10 上に記憶されているデータを破壊したり第三者に勝手に送信する可能性はないか、などをチェックする。その結果、問題なければ、実行プログラムファイルに署名を付加する。

30

【0041】

コンテンツ登録管理機能は、受け付けたコンテンツをシステム全体で一意に特定するコンテンツ ID を生成し、その ID 毎にコンテンツの有効性をデータベースを用いて管理する機能であり、コンテンツ登録者がコンテンツを登録する際にデータベースにコンテンツ登録情報を新規追加する機能と、登録したコンテンツの有効性が失われた際にコンテンツ登録情報を「失効」に変更する機能と、有効期限切れのコンテンツ登録情報をデータベースから削除する機能とを備える。

40

更に、負荷分散のため署名検証サーバ装置 40 やコンテンツ登録サーバ装置 50 を複数台設置した際に、コンテンツ登録者が一台のコンテンツ登録サーバ装置 50 に対して申請処理を行うだけで、申請された結果が他サーバ装置に行き渡るようにするため、コンテンツ登録情報を他の装置に配布する機能を備える。

【0042】

この機能により、コンテンツ登録情報がコンテンツ登録サーバ装置 50 間で不整合が生じることを防ぎ、また、署名検証サーバ装置 40 で署名検証処理が発生した際に、毎回コンテンツ登録サーバ装置 50 に対するコンテンツ登録情報の問い合わせによるオーバーヘッドを回避できる。

50

【0043】

例えば、コンテンツ登録者があるコンテンツを一旦登録した後、登録コンテンツの削除申請を行ったとする。コンテンツ登録サーバ装置50は、まずコンテンツ登録者端末装置80からコンテンツの登録を受け付け、コンテンツ検証サーバ装置60で内容チェックした後、そのコンテンツに対してIDを割り振り、データベースに新規に「有効」コンテンツとして登録し、署名検証サーバ装置40及び他のコンテンツ登録サーバ装置50上のデータベースに対して更新処理する。

【0044】

コンテンツ登録者端末装置80から上記コンテンツの削除申請があった場合、有効期限内のコンテンツであれば「失効」状態に変更し、有効期限切れであれば、データベースに格納されている上記コンテンツの情報を削除する。そして、先と同様に署名検証サーバ装置40及び他のコンテンツ登録サーバ装置50上のデータベースに対して更新処理する。

10

【0045】

クライアント装置10から削除申請のあったコンテンツにアクセスがあれば、署名検証サーバ装置40は、通信プロキシ装置20から送られてきた署名付きコンテンツ31の署名の有効性を検証した後、署名中のコンテンツIDを確認する。そのコンテンツIDをキーとして、内部のコンテンツ登録情報のデータベースを検索した後、コンテンツの状態が「失効」になっているか削除されている事を確認すると、そのコンテンツの検証結果が無効だとして、クライアント装置10に送信しないよう通信プロキシ装置20に通知する。

【0046】

コンテンツ検証サーバ装置60は、コンテンツ登録サーバ装置50から送信されたコンテンツの内容をチェックし、クライアント装置10にそのコンテンツを送信しても良いかどうかをチェックして、その結果をコンテンツ登録サーバ装置50に応答する。例えば、コンテンツ中のウィルス感染や、プログラムが使用するために読み込んでいるクラスライブラリがクライアント端末10上に記憶されているデータを破壊したり第三者に勝手に送信する可能性のあるものか、等を解析する。

20

【0047】

認証局70は、失効証明書リスト(CRL)を、定期的に、もしくは要求があった時に、署名検証サーバ40に配布する。

【0048】

コンテンツ登録者端末装置80は、コンテンツ作成者、コンテンツ保持者、コンテンツ提供者等のコンテンツ管理者がコンテンツ登録サーバ装置50にコンテンツを登録するのに用いる装置であり、コンテンツ管理者が、コンテンツ及び登録者情報等の登録申請もしくは削除申請するためのユーザインタフェース機能と、コンテンツ登録サーバ装置50に対する通信機能とを備える。

30

【0049】

コンテンツ登録者端末装置80は、Webブラウザが起動している端末でよい。コンテンツ登録者は、Webブラウザを起動し、コンテンツ登録サーバ装置50にアクセスし、応答としてWebブラウザに表示された入力フォームに登録者情報等の必要事項、及びコンテンツ登録者端末装置80に記憶されている登録対象のコンテンツのファイルパス(ディスク上の位置情報)を入力して、『登録』ボタンを押すと、コンテンツ登録者端末80から、コンテンツ登録サーバ装置50に対して、コンテンツ登録申請情報とコンテンツの電子データが送信される。その後、コンテンツ登録サーバ装置50からの応答として、登録申請時であれば、登録処理結果が画面に表示され、署名が付加されたコンテンツがダウンロードされる。

40

【0050】

削除申請時であれば削除処理結果が画面に表示される。登録処理や削除処理に失敗した場合はエラーメッセージが応答される。コンテンツ登録者は、応答された署名付きコンテンツ31をサーバ装置30のハードディスクなどの記憶装置に格納する。この時、署名付きコンテンツ31をコンテンツ登録者端末装置80からサーバ装置30に移し変えるには、

50

一旦署名付きコンテンツ 31 をフレキシブルディスク等の記憶媒体に格納して行う方法や、サーバ装置 30 とコンテンツ登録者端末装置 80 との間にセキュアな通信経路で行う方法がある。

【0051】

図 1 に示す構成において、複数の装置で実現されている機能が、物理的に一つの装置で実現されていても良い。例えば、署名検証サーバ装置 40 の機能が、通信プロキシ装置 20 に含まれていても良い。また、一つの装置で実現されている機能が、物理的に複数の装置で実現されていても良い。例えば、コンテンツ登録サーバ装置 50 の署名発行機能とコンテンツ登録管理機能とがネットワーク経由で互いに通信する別々のサーバ装置で実現されても良い。

10

【0052】

図 2 ないし図 14 を用いて、第一の実施形態を説明する。

【0053】

図 2 は、本実施の形態の通信プロキシ装置 20 の一構成図である。

【0054】

本実施の形態の通信プロキシ装置 20 は、データ通信を中継する通信中継処理部 21 と、通信データを署名検証サーバ装置 40 に転送するための条件情報が記憶されている転送制御データベース 22 と、署名検証サーバ装置 40 と接続するためのアプリケーションサーバ呼び出し処理部 23 とを備える。

【0055】

通信中継処理部 21 は、クライアント装置 10 から送信されてきたアクセス要求を受信し、アクセス要求中の URL 情報に示されるサーバ装置 30 に転送する。また、サーバ装置 30 から応答された署名無しのコンテンツを受信し、クライアント装置 10 に転送する。

20

【0056】

通信中継処理部 21 は、署名付きコンテンツ 31 受信時に、転送制御データベース 22 に記憶されている条件情報に基づき、署名検証サーバ装置 40 に署名付きコンテンツ 31 を送信するため、アプリケーションサーバ呼び出し処理部 23 に未検証の署名付きコンテンツ 31 を渡す。その後、署名検証サーバ装置 40 の検証結果として「検証成功」もしくはオリジナルコンテンツ 311 が応答された場合は、オリジナルコンテンツ 311 をクライアント装置 10 に応答する。また、署名付きコンテンツ 31 の状態で応答された場合は、署名 312 を除去したオリジナルコンテンツ 311 を、もしくは署名付きコンテンツ 31 をそのままクライアント装置 10 に応答する。ここで、署名を除去するか否かは、通信プロキシ装置 20 の設定による。「検証失敗」であれば、クライアント装置 10 に対してエラー通知する。ここで、オリジナルコンテンツ 311 以外のコンテンツが応答された場合は、受信したコンテンツをそのままクライアント装置 10 に送信しても良い。

30

【0057】

転送制御データベース 22 は、図 3 に示す転送条件フィールド 221 を検索キーとしたテーブル形式のデータベースで、署名検証サーバ装置 40 に署名付きコンテンツ 31 を転送する条件を管理するために使用する。転送制御データベース 22 の各エントリ 225 の内、転送条件フィールド 221 は、署名検証サーバ装置 40 に署名付きコンテンツ 31 を転送するトリガとなる条件情報を記憶する。転送先 URL フィールド 222 は、転送条件フィールド 221 にマッチした時に、署名付きコンテンツ 31 を署名検証サーバ装置 40 に送信するための宛先 URL を記憶する。サービス名フィールド 223 は、転送条件フィールド 221 にマッチした時に発動されるサービスの名称を記憶する。タイミングフィールド 224 は、転送条件フィールド 221 にマッチした時に、どの時点で署名検証サーバ装置 40 に送信する処理を発動させるか、といった情報を記憶する。

40

【0058】

例えば、図 3 のエントリ 225 で示される例では、転送条件フィールド 221 に「拡張子 = ".exe"」とあるので、クライアント装置 10 から受信したアクセス要求の宛先 URL のファイルの拡張子が ".exe" であるときに、条件にマッチする。マッチしたデ

50

ータ通信において、「ウィルススキャン」サービスとして、サーバ装置30から「コンテンツを受信した後」に、URL「http://web service1/virus_scan.cgi」で指示される署名検証サーバ40に署名付きコンテンツ31を転送する。

【0059】

また、署名中に、署名検証サーバ装置40のURLを記述しておいて、署名付きコンテンツ31を受信した際に、署名中に記載されたURLに指示される署名検証サーバ装置40に転送してもよい。

【0060】

図2のアプリケーションサーバ呼び出し処理部23は、署名検証サーバ装置40に署名付きコンテンツ31を送信する際に、署名検証サーバ装置40と接続を確立し、署名付きコンテンツ31を含むメッセージ32を作成する。メッセージ32は、例えば、図9に示す署名付きコンテンツ31に、クライアント装置10によるアクセス要求中に記述されていて、通信プロキシ装置20が保存しているアクセス先URL情報321を付加して構成する。アクセス先URL情報321を用いることで、署名検証サーバ40で署名を検証する際に、この署名付きコンテンツ31が本来置かれているべきURLからダウンロードされているかどうかをチェックすることが可能となる。

【0061】

図4は、署名検証サーバ装置40の一構成例を示す。

【0062】

署名取得部41は、通信プロキシ装置20から送信されたメッセージ32を解析し、未検証の署名付きコンテンツ31を取得する。そして、該コンテンツ31に付加されている署名312を取得すると共に、署名312の有効性を検証するために必要な、該コンテンツ31の署名312中に付加されている公開鍵証明書3123を取得して、該公開鍵証明書3123を検証するために、証明書検証部42に渡す。

【0063】

検証結果、該公開鍵証明書3123が有効であれば、証明書検証部42から公開鍵を取得する。取得した署名312及び公開鍵を署名検証部44に渡し、その結果として、署名312の検証結果を得る。この検証結果、該コンテンツ31が「有効」とであると確認されたならば、通信プロキシ装置20に対する応答として、「検証成功」を通知する。また、その時に、通信プロキシ装置20に対して検証成功したオリジナルコンテンツ311、もしくは署名付きコンテンツ31を送信しても良い。

【0064】

該公開鍵証明書が無効で、証明書検証部42から検証失敗が応答された場合、もしくは、署名検証部44の検証結果、該コンテンツ31が「無効」もしくは「失効」であった場合には、通信プロキシ装置20に「検証失敗」を通知する。また、その際、該コンテンツのコンテンツ登録者に対して、サーバ装置30から該コンテンツを削除するように依頼する旨のメール通知を行う機能を追加しても良い。

【0065】

証明書検証部42は、認証局70から定期的に、もしくは必要に応じて失効証明書リスト(CRL)を受信し、失効証明書リストデータベース43に登録し、管理する。また、署名取得部41から公開鍵証明書3123を渡されると、まず、公開鍵証明書が有効期限切れで失効していないかどうかをチェックする。その次に、失効証明書リストデータベース43を参照して、該公開鍵証明書3123が失効していないかどうかをチェックする。該公開鍵証明書3123が有効であると判明すると、署名取得部41に、処理結果として、該公開鍵証明書3123中に格納されている公開鍵を渡す。また、無効であれば、検証失敗を通知する。

【0066】

署名検証部44は、署名取得部41から署名312及び公開鍵を渡されると、署名312の検証を行う。また、署名32中のコンテンツID3125を登録情報管理部46Aに渡

10

20

30

40

50

して、該コンテンツの登録状態を検索する。検索結果、該コンテンツの登録状態が有効であれば、署名取得部 41 に「有効」通知する。また、無効、もしくは失効であれば、「無効」通知する。

【0067】

登録情報データベース 45A は、コンテンツ ID 3125 を検索キーとした、テーブル形式のデータベースで、コンテンツ登録状態を管理するために使用する。コンテンツ登録状態とは、そのコンテンツが「有効」（＝クライアント装置 10 に応答しても良い）か「失効」（＝クライアント装置 10 に応答してはいけない）かを表す状態のことを指す。「有効」状態は、そのコンテンツがコンテンツ登録サーバ装置 50 に登録済みで、かつ有効期限内であるときに設定される。「失効」状態は、そのコンテンツがコンテンツ登録サーバ装置 50 に登録済みで、かつ有効期限内であるが、コンテンツ登録サーバ装置 50 に対して削除申請がなされたときに設定される。なお、有効期限切れ、もしくはコンテンツ登録サーバ装置 50 に登録申請がなされていない（＝登録状態データベース 45A に登録されていない）コンテンツの場合は「無効」扱いとする。

10

【0068】

「失効」と「無効」との違いを、署名検証サーバ装置 40 及び通信プロキシ装置 20 の出力するログ内容や、クライアント装置 10 に応答するメッセージ内容、またはコンテンツ登録者に対するメール通知内容などに反映しても良い。

【0069】

登録情報データベース 45A の一構成例を図 5 に示す。

20

【0070】

コンテンツ ID フィールド 451 は、本システム内で各登録済みコンテンツに一意に割り振られたコンテンツ ID 3125 を記憶する。登録状態フィールド 452 は、前述したコンテンツの登録状態情報を記憶する。有効期限フィールド 453 は、登録済みコンテンツの登録状態の有効期限情報を記憶する。この有効期限を超過したコンテンツは無効となり、コンテンツ登録者によって再登録（更新）処理が必要となる。

【0071】

URL フィールド 454 は、登録コンテンツのネットワーク上の位置を示す情報である URL 情報を記憶する。登録者情報フィールド 455 は、コンテンツを登録した登録者の住所氏名やメールアドレスなどの個人情報を記憶する。失効日時フィールド 456 は、コンテンツ登録サーバ装置 50 に対してコンテンツの削除申請がなされた際に、その削除処理受け付け完了日時を記憶する。セキュリティレベルフィールド 457 は、後述するコンテンツ検証サーバ装置 60 での処理に用いるセキュリティレベル情報を記憶する。

30

【0072】

図 4 の登録情報管理部 46A は、登録情報データベース 45A に対して、データベースの検索や更新を行う。署名検証部 44 から、あるコンテンツ ID 値に対する検索要求が渡されると、登録情報データベース 45A を検索して、そのコンテンツ ID 3125 の登録状態フィールド 452 に記憶されている情報から、そのコンテンツの登録状態を判定して「有効」、「失効」、または「無効」を署名検証部 44 に通知する。また、コンテンツ登録サーバ装置 50 から登録情報の更新（登録及び削除）要求を受信すると、その内容に応じて登録状態データベース 45A の内容を更新する。さらに、署名検証サーバ装置 40 が内部に登録情報データベース 45A を記憶しておらず、他サーバ装置が一括管理をしている場合は、そのサーバ装置が、コンテンツ ID 3125 と共に、ネットワーク経由で登録情報検索依頼を送信しても良い。

40

【0073】

図 6 に、コンテンツ登録サーバ装置 50 の一構成例を示す。

【0074】

コンテンツ登録処理部 51 は、コンテンツ登録者端末装置 80 からアクセス要求を受信すると、必要事項を入力するための入力フォーム画面を応答し、コンテンツの登録及び削除申請を受け付ける。次に、コンテンツ登録者端末装置 80 から登録者情報などの必要事項

50

、及びオリジナルコンテンツ 311 を受信する。登録申請を受け付けた際には、コンテンツ検証サーバ装置 60 に登録申請されたオリジナルコンテンツ 311 を送信し、コンテンツの内容について検証処理を依頼する。検証結果に問題なければ、登録情報管理部 46B に登録要求を出し、コンテンツ ID 3125 を取得する。さらに、オリジナルコンテンツ 311 及び取得したコンテンツ ID 3125 を署名生成部 52 に渡し、署名付きコンテンツ 31 を取得した後、処理結果及び該署名付きコンテンツ 31 を、コンテンツ登録者端末装置 80 に応答する。削除申請を受け付けた際には、コンテンツ登録者端末装置 80 からコンテンツ ID 3125 もしくは URL 情報を入力してもらうことで、登録情報管理部 46B に、該コンテンツ ID 3125 もしくは該 URL 情報を検索キーとして、該コンテンツに対応するエントリを検索し、削除する。

10

【0075】

署名生成部 52 は、コンテンツ ID 3125 を渡されることで、図 9 に示される、署名付きコンテンツ 31 を作成する。その際、鍵管理部 53 が安全に記憶している、署名生成に必要な秘密鍵、公開鍵証明書 3123 を得る。

【0076】

登録情報管理部 46B は、基本的には図 4 に記載の登録情報管理部 46A と同じものである。追加機能として、コンテンツ登録要求を受けると、登録情報データベース 45B に対して、新規エントリの作成を行い、未使用のコンテンツ ID 3125 を割り振る。また、コンテンツ ID 3125 もしくは URL 情報と共にコンテンツ削除要求を受けると、登録情報データベース 45B に対して、渡された該コンテンツ ID 3125 もしくは URL 情報を検索キーとしてエントリを検索し、マッチしたエントリを削除する。

20

【0077】

さらに、登録情報管理部 46 は、コンテンツの登録、削除処理が行われた際に、他のコンテンツ登録サーバ装置 50 及び署名検証サーバ装置 40 が有する登録情報データベース 45 に対して、ネットワーク経由で通信を行い、登録、削除処理を行う機能を有する。本機能により、データベースの内容の整合性を保証することが可能となる。登録情報データベース 45B は、図 5 に記載の登録情報データベース 45A と同じものである。

【0078】

図 7 に、登録情報管理部 46 間で、ネットワークを介して登録情報データベース 45 の内容を同期させる方法の一例を示す。コンテンツ登録サーバ装置 50 を複数設置しているケースでは、登録情報データベース 45 の内容の同期が重要な問題となる。内容の不一致やコンテンツ ID 3125 の重複を回避するため、常に最新情報を記憶する登録情報データベース 45 を用意し、コンテンツ登録サーバ装置 マスタ 50A と位置付ける。他のコンテンツ登録サーバ装置 50B (スレーブという) にコンテンツ登録申請があると、コンテンツ登録処理部 51B から登録情報管理部 46B に登録要求が渡される。次に、ネットワーク通信を行うことで、コンテンツ登録サーバ装置 マスタ 50A に登録要求を渡し、割り当てられたコンテンツ ID 3125 を取得する。このコンテンツ ID 3125 を用いて登録情報データベース 45B を更新し、署名を 312 を生成することで、コンテンツ登録サーバ装置 50 間でのコンテンツ ID 3125 の重複を回避して共有することが可能となる。

30

【0079】

図 8 に、コンテンツ検証サーバ装置 60 が備える、実行プログラムファイルの内容検証に用いるテーブル形式のデータベースを例示する。

40

【0080】

このデータベースは、実行プログラムファイルが使用する関数や、読み込むクラスライブラリに基づいてセキュリティレベルを決定するために使用する。エントリ 620 は、プログラムの安全度を表すセキュリティレベルフィールド 611、関数名フィールド 612 ~ 614、クラスライブラリ名フィールド 615 ~ 617 を備える。図 8 の例は、関数 1 を使用しているプログラムと、クラスライブラリ 1 を読み込んでいるプログラムは、セキュリティレベル 2 であることを示している。

【0081】

50

コンテンツ検証サーバ装置 60 が、コンテンツ検証時に上記データベースを参照して決定したセキュリティレベルと、コンテンツ登録者が登録した図 5 の登録情報データベース 45 のセキュリティレベルフィールド 457 の値を比較することで、本システムの運用者とコンテンツ登録者間で結ばれた契約の内容に応じた安全度のコンテンツの配布が可能となる。例えば、高い契約料を本システム運用者に支払っているコンテンツ登録者 A は、安全度の低いプログラムも配布することができるが、安い契約料を支払っているコンテンツ登録者 B は、安全度の高いプログラムのみしか配布できない、というような運用が可能となる。

【0082】

図 10 に、コンテンツ登録サーバ装置マスタ 50 A における、コンテンツ登録申請処理の処理フロー例を図示する。 10

【0083】

まず、コンテンツ登録者が、コンテンツ登録者端末装置 80 において、Web ブラウザなどで登録者情報 455 を含む必要事項を入力し (S501)、コンテンツ登録サーバ装置マスタ 50 A に対し、必要事項及びオリジナルコンテンツ 311 を送信する (S502)。コンテンツ登録処理部 51 が該登録者情報 455 を含む必要事項及び該コンテンツ 311 をコンテンツ登録者端末装置 80 から受信した後、該コンテンツ 311 をコンテンツ検証サーバ装置 60 に送信する (S503、S504)。コンテンツ検証サーバ装置 60 でコンテンツ検証を行った後 (S505)、コンテンツ検証サーバ装置 60 は検証結果を応答する (S506)。 20

【0084】

応答されたコンテンツ検証結果をチェックし (S507)、問題が無ければ (例えば、プログラムにウィルスが含まれていない、セキュリティの低い関数が使われていない、など)、登録情報管理部 46 B により、未使用のコンテンツ ID 3125 を割り当てる (S510)。次に、署名生成部 52 により、署名 312 を生成する (S511)。次に、登録情報データベース 45 B に新規エントリ 459 を作成する (S512)。さらに、登録情報管理部 46 B が、署名検証サーバ装置 40 及び他のコンテンツ登録サーバ装置 50 に対して、登録情報の更新 (登録) 処理を行う (S513~S5015)。最後に、コンテンツ登録者端末装置 80 に対し、コンテンツ登録処理部 51 が検証結果として「登録手続き完了」通知及び署名付きコンテンツ 31 を送信する (S516、S5017)。 30

【0085】

なお、S507 で検証結果に問題があった場合は、コンテンツ登録処理部 51 は、コンテンツ登録者端末装置 80 に対して、検証結果として「コンテンツ検証失敗」の旨の通知を送信する (S508、S509)。

【0086】

図 11 に、スレーブのコンテンツ登録サーバ装置 50 B における、コンテンツ登録申請処理の処理フロー例を図示する。

【0087】

S501 から S509 までは図 10 と同じである。S507 以降、コンテンツ登録サーバ装置マスタ 50 A への登録処理が行われる (S601)。該登録者情報 455 及び該コンテンツ 31 をコンテンツ登録サーバ装置マスタ 50 A に送信し (S602)、コンテンツ ID 3125 の発行 (S603)、及び登録情報データベース 45 B の更新を行い (S604)、コンテンツ登録サーバ装置 50 B にコンテンツ ID 3125 を渡す (S605)。S605 以降の処理については、図 10 の S511 から S517 の処理と同じである。 40

【0088】

図 12 に、コンテンツ登録サーバ装置 50 における、コンテンツ削除申請処理の処理フロー例を図示する。

【0089】

まず、コンテンツ登録処理部 51 が、削除申請の対象コンテンツの URL もしくはコンテンツ ID 3125 をコンテンツ登録者端末装置 80 から受信した後、登録情報管理部 46 50

Bが該コンテンツを登録情報データベース45Bから検索する(S201)。削除コンテンツが存在するかチェックし(S202)、存在していれば、有効期限フィールド453をチェックし、有効期限内かどうかをチェックする(S203)。有効期限内であれば、登録状態452を「失効」に変更する(S204)。また、有効期限外であれば、エントリ459そのものを削除する(S205)。その次に、登録情報管理部46Bが、署名検証サーバ装置40及び他のコンテンツ登録サーバ装置50に対して、登録情報の更新(削除)処理を行う(S206)。最後に、コンテンツ登録者端末装置80に対し、コンテンツ登録処理部51が検証結果として「失効手続き完了」通知を送信する(S207)。また、処理S202で削除コンテンツが存在しなければ、コンテンツ登録処理部51が、コンテンツ登録者端末装置80にエラーメッセージを通知する(S208)。

10

【0090】

次に、コンテンツ登録サーバ装置50で定期的に発生する、登録情報データベース45の有効期限チェック処理フロー例について説明する。

【0091】

まず、登録情報管理部46が、登録情報データベース45のエントリ459を参照し、未参照エントリが存在するかどうかをチェックする。存在していれば、有効期限フィールド453を参照し、有効期限を超過しているかどうかをチェックする。有効期限を超過していれば、該エントリを削除する。有効期限内であれば、削除しない。他にエントリ459があれば上記処理を繰り返し、未参照エントリが存在しなければ、登録情報管理部46Bが、署名検証サーバ装置40及び他のコンテンツ登録サーバ装置50に対して、登録情報の更新処理を行う。

20

【0092】

図13に、クライアント装置10から署名付きコンテンツ31に対してアクセス要求があった際の処理フロー例を図示する。

【0093】

まず、クライアント装置10から通信プロキシ装置50に対してアクセス要求が送信される(S701、S702)と、通信プロキシ装置50でアクセス対象コンテンツのキャッシュを記憶しているかどうかを確認し(S703)、キャッシュがあれば、クライアント装置10にキャッシュを送信する(S704、S705)。キャッシュがなければ、アクセス要求をサーバ装置30に転送する(S706)。

30

【0094】

サーバ装置30が署名付きコンテンツ31を通信プロキシ装置20に応答後(S707、S708)、通信プロキシ装置20は該コンテンツ31を署名検証サーバ装置40に転送する(S709、S710)。署名検証サーバ装置40は付加処理として署名の検証処理を行った後、結果を通知する(S711、S712)。このとき、結果通知と共に、検証済みのオリジナルコンテンツ311か、署名付きコンテンツ31か、もしくはエラーメッセージを通信プロキシ装置20に送信しても良い。

【0095】

その後、通信プロキシ装置20は、検証済みのオリジナルコンテンツ311か、署名付きコンテンツ31か、もしくはエラーメッセージをクライアント装置10に送信し(S713、S714)、キャッシュ可能であれば、キャッシュとしてオリジナルコンテンツ311、もしくは署名付きコンテンツ31を保存する(S715)。

40

【0096】

なお、S711、S712の処理で署名付きコンテンツ31が送られた場合、通信プロキシ装置20のS713での処理において、署名付きコンテンツ31から署名312を除去して、オリジナルコンテンツ311をクライアント装置10に送信しても良い。また、署名検証サーバ装置40で付加処理されたオリジナルコンテンツ311に別のコンテンツのURLが記載されていた場合に、そのURLに記載されたURLに改めてアクセスして、受信したコンテンツをクライアント装置10に送信しても良い。

【0097】

50

なお、コンテンツ登録申請処理が行われた際に、コンテンツ登録サーバ装置 50 が通信プロキシ装置 20 の通信中継処理部 21 に対し、検証済みコンテンツをキャッシュするように指示してもよい。この場合、コンテンツ登録サーバ装置 50 が登録したコンテンツが直ぐに通信プロキシ装置 20 のキャッシュに格納されるため、クライアント装置 10 からこのコンテンツにアクセスがあると、キャッシュから削除されない限りは必ずキャッシュから応答されるため、高速な応答を行うことができるという利点がある。

【0098】

図 15 に示す第 2 の実施の形態では、通信プロキシ装置 20 が多段になっており、クライアント装置 10 とクライアント装置 10 に各々最寄の通信プロキシ装置 20 A、20 B 間には暗号化された通信路 901 が確立されている。

10

【0099】

本実施の形態では、キャッシュを用いてクライアント装置 10 に高速に応答する通信プロキシ装置 20 A と、サーバ装置 30 の近くの通信プロキシ装置 20 B と署名検証サーバ装置 40 を分けて運用するため、機能分散の効果があり、システム全体の負荷を分散することが可能となる。また、通信プロキシ装置 20 A を通信キャリアが保有し、通信プロキシ装置 20 B を企業やコンテンツ提供者が保有するなど、通信プロキシ装置 20 の備える機能ごとに、運用の分担を行うことが可能となる。

【0100】

次に第 3 の実施の形態として、本発明のネットワークシステム及びコンテンツ検証方法を用いたコンテンツダウンロードのフローの一例を示す。PC や携帯電話が、ネットワーク経由でコンテンツをダウンロードする際、以下のようなシーケンスで行なう。

20

【0101】

本体のコンテンツをダウンロードする前に、コンテンツ本体の URL 等の補助情報が記述されているメタデータと呼ばれるファイルをダウンロードする。次に、メタデータに記述されている情報を解釈して得られた情報を基にコンテンツ本体をダウンロードし、実行する。

【0102】

本実施形態では、メタデータ中にコンテンツ本体の署名を付加する。メタデータは、メタデータ自身の署名と、メタデータと対になるコンテンツの署名の両方を備える。署名検証サーバ装置 40 は、メタデータのダウンロード時にコンテンツ用の署名を保存しておき、その後のコンテンツダウンロード時に、保存していた署名でコンテンツを検証する。

30

【0103】

メタデータとコンテンツ本体の URL の対応付けは、コンテンツ登録サーバ 50 での登録時に行う。署名検証サーバ装置 40 は、この対応付け情報をコンテンツ登録サーバ 50 から受信し、テーブルで管理する。また、この対応付けテーブルを用いて、メタデータに付加されているメタデータ自身の署名とコンテンツの署名の記憶場所も管理する。このテーブルに管理されている以外の URL のメタデータやコンテンツが転送されてきた場合は、署名検証サーバ装置 40 は不正アクセスのエラーとして処理する。さらに、コンテンツ用の署名の記憶期限を予め署名検証サーバ装置 40 に設定しておけば、サーバ装置のメモリ資源の無駄な消費を防ぐことが出来る。

40

【0104】

図 16 を用いて説明する。クライアント装置 10 から通信プロキシ装置 50 に対してメタデータへのアクセス要求が送信される (S801) と、通信プロキシ装置 50 でアクセス先のコンテンツのキャッシュを記憶しているかどうかを確認し、キャッシュがあれば、クライアント装置 10 にキャッシュを送信する (S802)。キャッシュがなければ、アクセス要求をサーバ装置 30 に転送する (S803)。

【0105】

サーバ装置 30 が署名付きメタデータを通信プロキシ装置 20 に応答後 (S804)、通信プロキシ装置 20 は該メタデータを署名検証サーバ装置 40 に転送する (S805)。署名検証サーバ装置 40 でメタデータの署名の検証処理を行い、メタデータとコンテンツ

50

の両方の署名を保存して、その記憶場所を対応付けテーブルに登録した後（S 8 0 6）、結果を通知する（S 8 0 7）。その後、通信プロキシ装置 2 0 は、検証済みのメタデータもしくはエラーメッセージをクライアント装置 1 0 に送信し（S 8 0 8）、キャッシュ可能であれば、キャッシュとしてメタデータを保存する（S 8 1 0）。

【0106】

クライアント装置 1 0 は、受信したメタデータの内容を解析した後（S 8 0 9）、通信プロキシ装置 5 0 に対して、メタデータ中で指示されたコンテンツへのアクセス要求を送信する（S 8 1 1）。通信プロキシ装置 5 0 で（既に署名検証済みの）コンテンツのキャッシュを記憶しているかどうかを確認し、キャッシュがあれば、クライアント装置 1 0 にキャッシュを送信する（S 8 1 2）。キャッシュがなければ、アクセス要求をサーバ装置 3 0 に転送する（S 8 1 3）。サーバ装置 3 0 がコンテンツを通信プロキシ装置 2 0 に応答後（S 8 1 4）、通信プロキシ装置 2 0 は該コンテンツとアクセス先 URL 情報 3 2 1 とからなるメッセージ 3 2 を署名検証サーバ装置 4 0 に転送する（S 8 1 5）。 10

【0107】

署名検証サーバ装置 4 0 は、該コンテンツの URL をキーにして対応付けテーブルを検索し、該コンテンツの対になるメタデータのエントリで管理され、前回のメタデータダウンロードに保存しているコンテンツの署名を探す。このとき署名が記憶されていれば、コンテンツの検証処理を行い、（S 8 1 6）、結果を通知する。署名が行き臆されていなければエラーを通知する（S 8 1 7）。その後、通信プロキシ装置 2 0 は、検証済みのコンテンツもしくはエラーメッセージをクライアント装置 1 0 に送信し（S 8 1 8）、キャッシュ可能であれば、キャッシュとしてコンテンツを保存する（S 8 1 9）。 20

【0108】

本実施例において、署名検証サーバ装置 4 0 が複数ある場合、コンテンツ本体の検証は、対応するメタデータを検証した署名検証サーバ装置 4 0 で行う必要がある。そのため、通信プロキシ装置 2 0 は、コンテンツ本体を署名検証サーバ装置 4 0 に転送する際に、特定の署名検証サーバ装置 4 0 に転送するための処理を行う。具体的には、S 8 0 7 の処理時に、通信プロキシ装置 2 0 に応答するメタデータ中に記述されているコンテンツの URL や、コンテンツやメタデータを送る際に用いる HTTP ヘッダに格納されている HTTP セッションの状態情報（例えば cookie ヘッダ等）を、書き換えもしくは書き加えて、署名検証サーバを識別するための ID を付加する。 30

【0109】

例えば、コンテンツ URL 書き換えの場合は、“http://サーバA/メタデータ”を“http://サーバA/メタデータ?署名検証サーバ装置=01”のように書き換える。クライアント装置 1 0 は、S 8 1 1 においてその書き換えられた URL に対してリクエストを送信するため、通信プロキシ装置 2 0 は、コンテンツ本体のダウンロード時に、その URL の“?”以下に付加された“署名検証サーバ装置=01”の部分を解釈して、特定の署名検証サーバ装置 4 0 にコンテンツを転送する。

【0110】

cookie の場合は、“Set-Cookie2: 署名検証サーバ装置=01”というヘッダを通信プロキシ装置 2 0 と署名検証サーバ装置 4 0 間の HTTP 中のメッセージに付加しておく。通信プロキシ装置 2 0 がクライアント装置 1 0 から cookie ヘッダ“Cookie: 署名検証サーバ装置=01”が付加されたリクエストを受信すると、その cookie ヘッダを解釈することで、URL の場合と同様に、特定の署名検証サーバ装置 4 0 へのコンテンツ転送を実現することができる。また、通信プロキシ装置 2 0 は、メタデータを転送した署名検証サーバ装置 4 0 の情報を記憶しているので、通信プロキシ装置 2 0 がこの cookie ヘッダを付加してクライアント装置 1 0 に送信しても良い。 40

【0111】

本実施の形態の利点としては、以下の二点がある。

【0112】

第一に、コンテンツが正式なメタデータによりダウンロードされているかを検証することができる。メタデータにはコンテンツのURL情報が記述されており、クライアント装置10はメタデータを解釈してからコンテンツを呼び出す。しかし、メタデータとコンテンツで個別に検証していたのでは、第三者が勝手にコンテンツを呼び出すメタデータを書くケースもありうる。そのため、コンテンツ自体の署名をメタデータに付加することにより、正式なコンテンツとメタデータが対でダウンロードされているということを検証することができる。

【0113】

第二に、コンテンツ自体には手を加えないため、本発明のネットワークシステムを用いずにコンテンツをダウンロードしても、クライアント装置10での実行に支障がない。たとえば、携帯電話からのアクセスには本ネットワークシステムを介するが、PCからのアクセスは本ネットワークシステムを介さない構成における、署名付きのメタデータとコンテンツをダウンロードする場合、メタデータに余計なデータ（ここでは署名）が付加されていても、メタデータはあくまで補助データであり、メタデータ自身を実行するわけではないので、通常、ダウンロードした装置ではエラーとはせずに無視する。しかし、署名付きのコンテンツを実行させようとする、コンテンツとは無関係の余計なデータ（すなわち署名）が付加されているため、エラーになる可能性がある。本実施形態のようにコンテンツの署名をメタデータに付加しておくことにより、クライアント装置10でのエラーを回避することができる。

【0114】

【発明の効果】

本発明によれば、クライアント装置やサーバ装置に変更を必要とせずに、高速なまたは高機能なコンテンツ検証システムを実現することができる。

【図面の簡単な説明】

【図1】コンテンツ検証システムの一論理構成図。

【図2】通信プロキシ装置20の一機能構成図。

【図3】転送制御データベース22の一構成図。

【図4】署名検証サーバ装置40の一機能構成図。

【図5】登録情報データベース45の一構成図。

【図6】コンテンツ登録サーバ装置50の一機能構成図。

【図7】登録情報データベース45の同期処理の一例。

【図8】コンテンツ検証システム60の備えるセキュリティ管理テーブルの一例。

【図9】署名付きコンテンツ31の一構成図。

【図10】ネットワークシステムにおけるコンテンツ登録処理フローの一例。

【図11】ネットワークシステムにおけるコンテンツ登録処理フローの一例。

【図12】ネットワークシステムにおけるコンテンツ削除処理フローの一例。

【図13】ネットワークシステムにおけるコンテンツダウンロード時の処理フローの一例。

。

【図14】本発明における各装置を実現する情報処理装置の一構成図。

【図15】ネットワークシステムにおける他の実施形態の構成例。

【図16】コンテンツ検証方法における他の実施形態の処理フロー。

【符号の説明】

10…クライアント装置、20…通信プロキシ装置、30…サーバ装置、40…署名検証サーバ装置、50…コンテンツ登録サーバ装置、60…コンテンツ検証サーバ装置、70…認証局、80…コンテンツ登録者端末装置、21…通信中継処理部、22…転送制御データベース、23…アプリケーションサーバ呼び出し部、41…署名取得部、42…証明書検証部、43…失効証明書リストデータベース、44…署名検証部、45…登録情報データベース、46…登録情報管理部、51…コンテンツ登録処理部、52…署名生成部、53…鍵管理部、31…署名付きコンテンツ、311…オリジナルコンテンツ、312…署名、32…メッセージ、321…アクセス先URL情報、9…ネットワーク、10…情

10

20

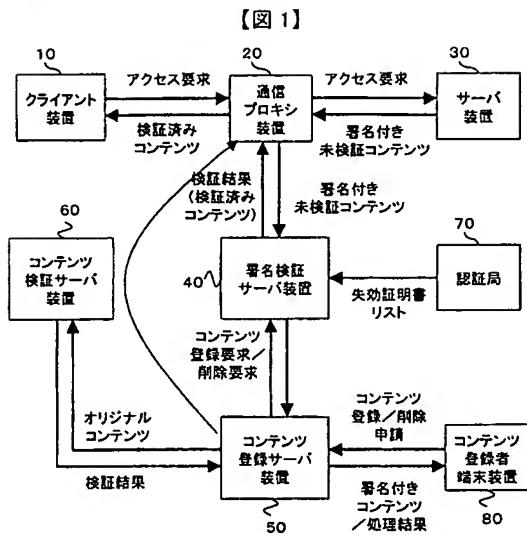
30

40

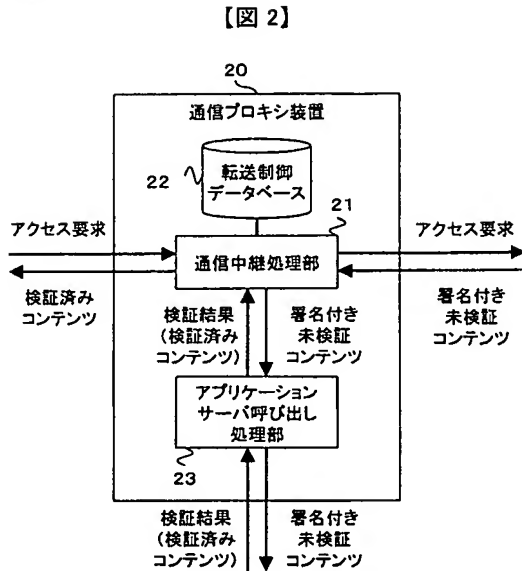
50

報処理装置、11…CPU、12…メモリ、13…読取装置、14…通信装置、15…外部記憶装置、16…入出力装置、17…内部バス、18…記憶媒体、901…暗号化通信路。

【図1】



【図2】



【図 3】

22

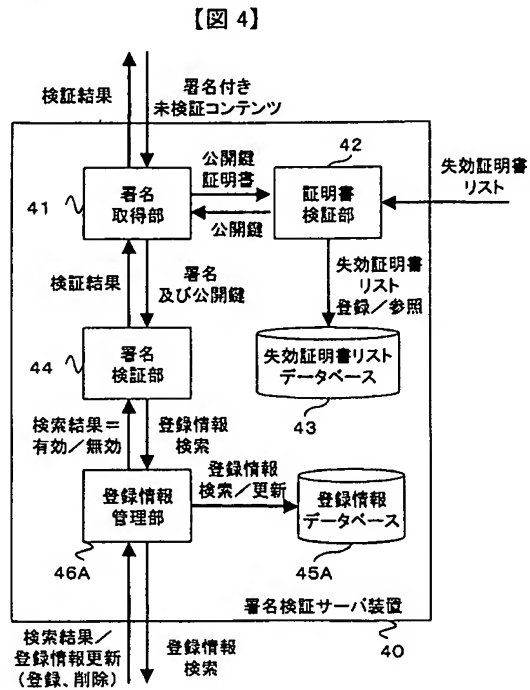
221	222	223	224
転送条件 フィールド	転送先URL フィールド	サービス名 フィールド	タイミング フィールド
拡張子=".exe"	http://webservice1/ virus_scan.cgi	ウイルススキャン	Webコンテンツ 受信後
拡張子=".jar"	icap://webservice2/ function_check	プログラム 関数チェック	Webコンテンツ 受信後
URL="http:// server1/A.mov"	icap://webservice3/ copyright_check	コンテンツ 改変チェック	Webコンテンツ 受信後
XMLタグ付き	タグに指示された URL	XMLタグ制御	Webコンテンツ 受信後

225

転送制御データベース

【図 3】

【図 4】



【図 5】

45

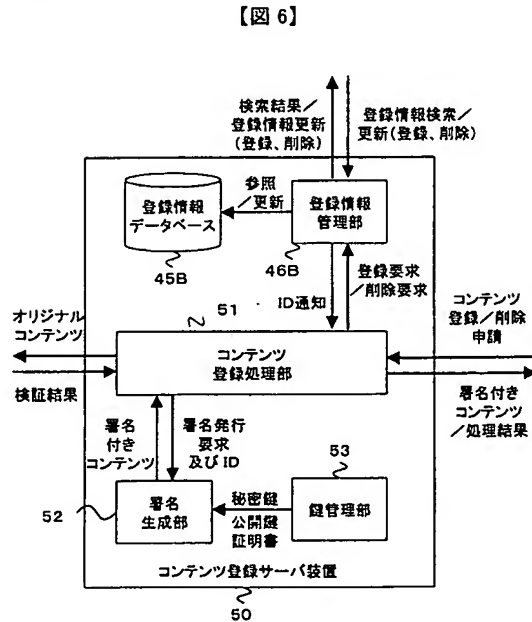
451	452	453	454	455	456	457
コンテンツ ID	登録状態	有効期限	URL	登録者 情報	失効日時	セキュリ ティ レベル
XXXXX1	有効	2003/1/1	http://URL1	USER1	-	2
XXXXX2	有効	2003/2/1	http://URL2	USER2	-	3
XXXXX3	失効	2003/3/1	http://URL3	USER3	2003/1/1	3

459

登録情報データベース

【図 5】

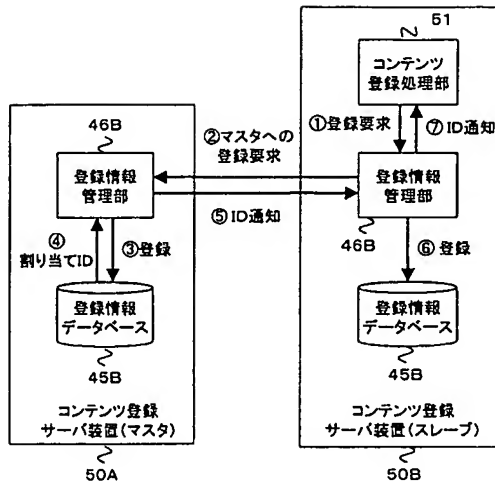
【図 6】



【図 6】

【図 7】

【図 7】



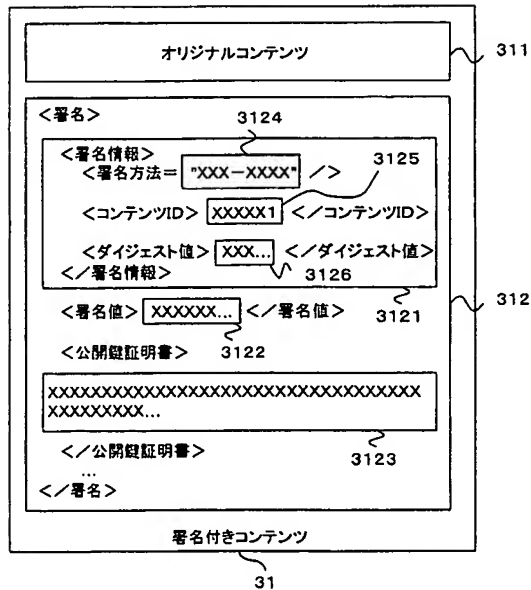
【図 8】

【図 8】

611	612	613	614	615	616	617
セキュリティ レベル	関数1	...	関数n	クラス ライブラリ1	...	クラス ライブラリn
1	x	x
2	o	x
2	x	o
...
n

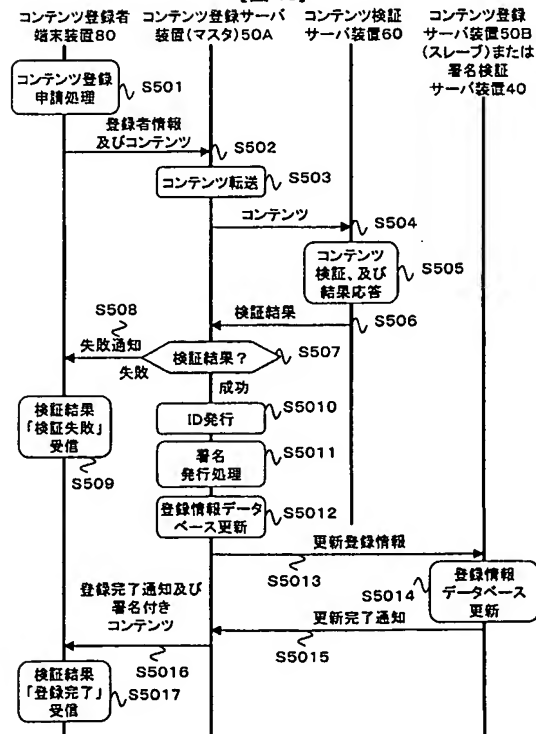
【図 9】

【図 9】

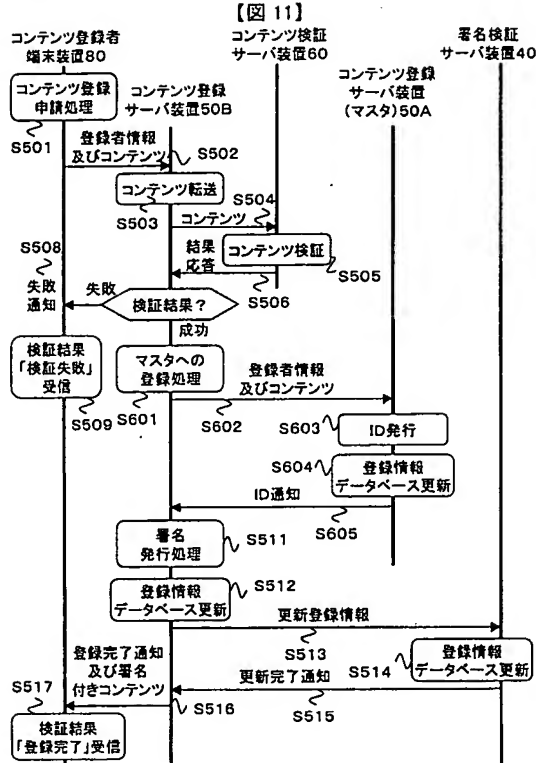


【図 10】

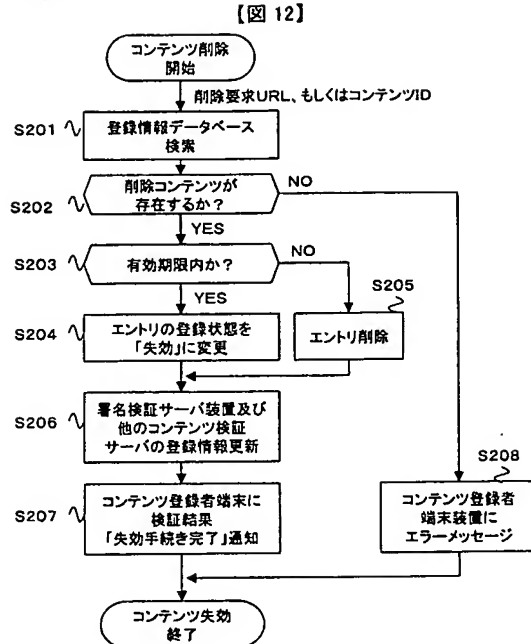
【図 10】



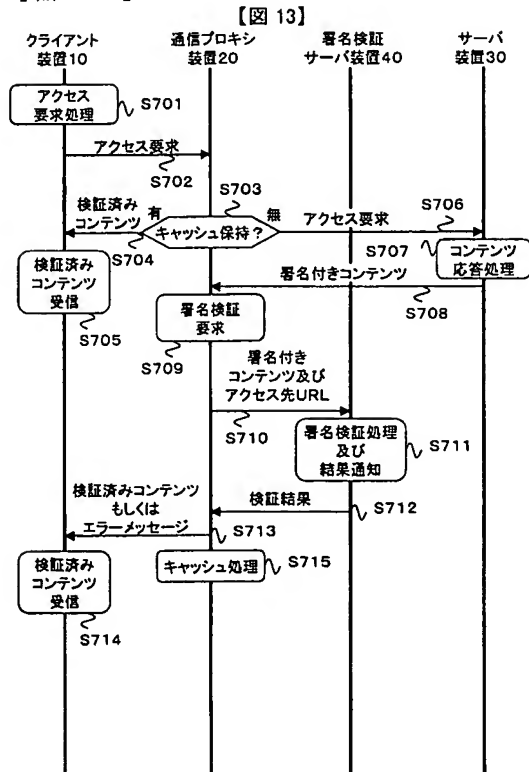
【図 11】



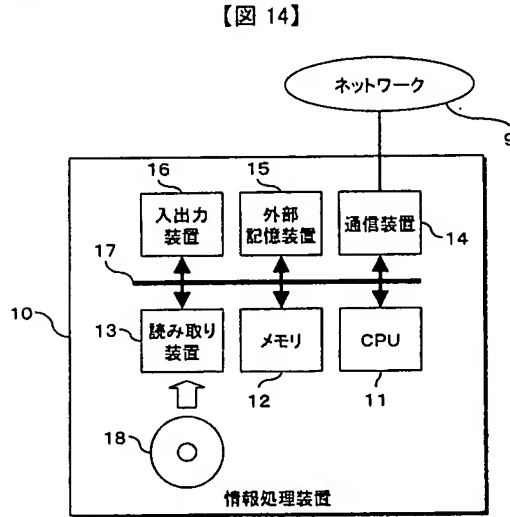
【図 12】



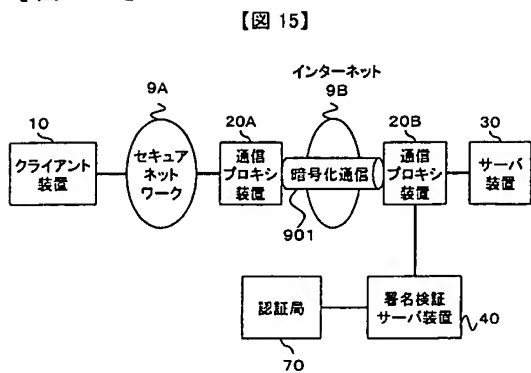
【図 13】



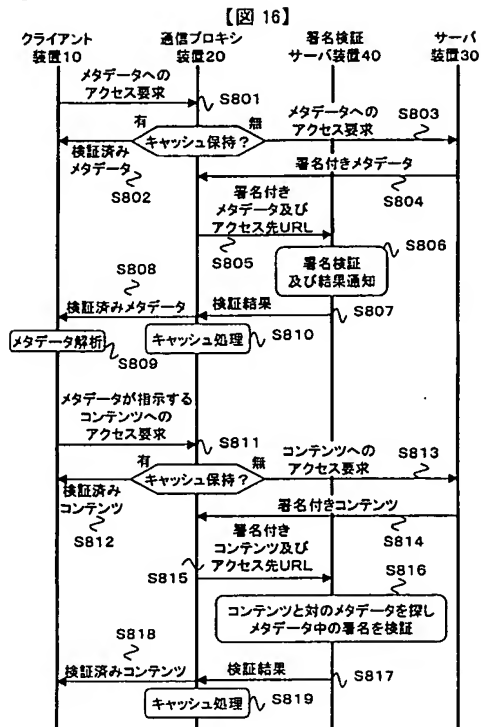
【図 14】



【図 15】



【図 16】



フロントページの続き

(51)Int.Cl.⁷

F I

テーマコード (参考)

H 0 4 L 9/00 6 7 5 D

F ターム (参考) 5B075 KK07 KK33 KK54 KK63 NK02 NR02 PP22

5B085 AE23 AE29 BG04 BG07

5J104 AA08 AA09 JA21 LA03 LA05 LA06 MA01 NA02 NA27 PA07